EXHIBIT 1

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**DECLARATION OF J. ALEX HALDERMAN IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION** **Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. I was present via teleconference for today's proceedings and heard the testimony of Dr. Eric Coomer and Mr. Gabriel Sterling regarding the State's intention to make unplanned, last-minute changes to the software that operates Georgia's BMDs. This surprise development alarms me, for several reasons.

3. First, changing voting equipment software on such short notice is far from routine, particularly barely a month before a Presidential election. This is

because altering the software risks unintentionally introducing new bugs, and it would provide an attractive vector for attackers seeking to spread malware.

4. Second, even if the intended changes are "de minimis" (as Dr. Coomer testified), meaning they involve differences in a small number of lines of source code, the update process necessitates completely replacing the most important part of the BMD's software. Dr. Coomer testified that Georgia must install a new "APK"—the Android application package that contains nearly all of each BMD's Dominion-authored software—onto each of some 33,000 machines across 159 counties. Given the accelerated timeline, there is no practical way to reliably inspect the APKs and determine that the only change to BMDs' functionality is the intended fix, or that the change does not introduce new bugs or even malicious behavior.

5. Third, in complex computerized systems like Georgia's election equipment, last-minute changes, even seemingly small ones, can introduce serious and difficult-to-foresee consequences. That is why rigorous testing of such changes is essential to ensure correct operation. An infamous recent example where such testing was cut short was the Boeing 737 Max aircraft. Boeing made a small last-minute software change to correct a single problem and inadvertently created a much

more dangerous failure mode that reportedly led directly to two fatal crashes.[1]

6. By analogy, what Dominion and Georgia are proposing to do is like redesigning an aspect of an airplane that is about to take off. The rapid deployment of this change will necessitate omitting or cutting short even the ineffectual testing and security measures used during the initial rollout of the BMDs. Unlike the software it replaces, the new software will not have been subject to EAC testing or Pro V&V's full Georgia certification tests. There also is no indication that it will undergo acceptance testing to confirm that the correct software has been installed. Although, as I previously testified, these steps have limited utility for security, they at least help guard against bugs and human error that could otherwise undermine results or render equipment inoperable on election day and during early voting. If the change does create unforeseen problems, the result would be hugely disruptive. There already is too little time to safely modify Georgia's BMD software *once* before the November election, and there is certainly not enough time to modify it *twice* if problems caused by the first change need to be corrected—especially if the problems are not discovered until election day.

---

[1] Jack Nicas, Natalie Kitroeff, David Gelles and James Glanz, "Boeing Built Deadly Assumptions Into 737 Max, Blind to a Late Design Change," *The New York Times* (June 1, 2019).

7. Finally, this last-minute software replacement compounds my previous concerns about the vulnerability of Georgia's BMD-based system. As I have already testified, malicious modifications to the BMDs' software could undermine the integrity of election results in multiple ways, including by changing either the barcodes alone or both the barcodes and the human readable text, with the result that election outcomes could be changed without detection. Replacing the software now, on the eve of the election, creates a vector by which an attacker could introduce malicious changes into BMDs state-wide. Malicious code could be introduced by what the defendants and their election experts often refer to as an "insider" at Pro V&V or by attackers who compromised the company's systems. It could also be introduced by modifying the software update package as it is being distributed to the state and onward to counties, or as the counties are copying it to machines across the state. As I previously testified, merely checking the hash of the software by using the BMDs' build-in features would not be sufficient to detect malicious alterations. The late-breaking nature of the change further increases the odds that such an attack would succeed, because whatever procedural protections are in place regarding software updates will need to be applied on a vastly accelerated basis involving every Georgia county, likely hundreds of personnel, and tens of thousands of machines.

8. I am especially perplexed that the State has decided to accept these risks, because it would appear, based on today's testimony, that simple procedural changes could correct the asserted problem without any changes to the software. Dr. Coomer characterized the user-interface problem as occurring only once each time a BMD is powered on and operated. If this is the case, the State should be able to simply instruct poll workers, after turning on each BMD, to print a test ballot and trigger the aberrant behavior before voters begin using the machine. By Dr. Coomer's description, the problem would not occur again until the BMD was rebooted. Dominion could correct the underlying software after the election, leaving time for a complete battery of critically important tests. That Georgia has chosen to accept the much greater risks of a last-minute software change suggests that the problem or problems being addressed may be more complex than has been described, making a hasty, untested fix all the more dangerous.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 28th day of September, 2020 in Ann Arbor, Michigan.

J. ALEX HALDERMAN